UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/690,017	10/21/2003	James P. Goddard	END920030107US1	4833

26502 7590 07/14/2011

IBM CORPORATION
IPLAW SHCB/40-3
1701 NORTH STREET
ENDICOTT, NY 13760

EXAMINER	
HOANG, DANIEL L	
ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
07/14/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

endiplaw@us.ibm.com

Office Action Summary	Application No.	Applicant(s)	
	10/690,017	GODDARD, JAMES P.	
	Examiner	Art Unit	
	DANIEL HOANG	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *2-9-11*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *38-49* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *38-49* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments, pertaining to the 103 rejections of the previous action are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Halligan, US PGP No. 20010044737.

CLAIMS PRESENTED

Claims 38-49 are presented.

CLAIM REJECTIONS

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 38-49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Voss, US Patent No. 7552480, and further in view of Halligan, US PGP No. 20010044737.

As per claims 38, 44:

A computer program product for evaluating a security risk of an application, the computer program product comprising:

> *[see col. 3, lines 15-20, "system for assessing and quantifying the risk exposure of an information system or application using a a one-dimensional quantitative risk assessment model.]*

one or more computer-readable tangible storage devices and program instructions stored on at least one of the one or more storage devices, the program instructions comprising;

program instructions to determine whether employees of two or more customer corporations are authorized to concurrently share use of the application;

> *[see col. 4, lines 23-32, wherein establishing the numerical value for the threat of attack involves establishing the potential for an attack on the information system asset by a threat agent and further wherein a threat agent is defined as casual users, kiddy scriptors, hackers, disgruntled employees, legitimate consumers, competitors, etc. Examiner understands this to mean that a threat value is calculated based on whether the application can be exploited by different users which is considered to be analogous to applicant's claim language of being shared by different customers.] see also col. 7-8]*

program instructions to determine whether a vulnerability in the application can be exploited by a user which has not been authenticated to the application;

> *[see col. 4, lines 42-52, wherein establishing a numerical value includes identifying one or more unauthorized privileges such as security administrator privileges] see also, col. 7-8]*

program instructions to assign numerical weights to the respective determinations, each of the numerical weights corresponding to a significance of the respective determination in quantifying the security risk; program instructions to combine the numerical weights to quantify the security risk; and

> *[see col. 4, lines 53-60, wherein the security risk level for the information asset is calculated as a product of the numerical value of the threat of attack times the numerical value for the access component of the vulnerability times the numerical value for the privilege component of the vulnerability to attack on the information system asset.]*

The Voss reference has been discussed above. While Voss teaches quantifying the security risks, Voss is mute in teaching comparing the quantified security risks with a monetary value of a benefit of the application. For this limitation, examiner relies on the Halligan reference. Halligan teaches a method wherein trade secrets are analyzed in order to calculate their value to the company. An analysis of the trade secret and its economic benefit factor are described in paragraphs 119-121. While the Halligan reference does not deal with security risks related to the adoption of an application by a company, Halligan does analyze the risks and benefits associated with sharing trade secrets. Examiner views that this is in a similar line as analyzing the risks and benefits of using an application which will allow customers to share access to private information. It would have been obvious to one of ordinary skill in the art to modify the Voss reference to compare the risk associated with the application with the economic

benefits that are associated with using the application. Doing so would let the company using the application know whether or not it is worthwhile to use the application even though possible risks exist.

As per claim 39, 45:

The computer program product of claim 38 further comprising:

program instructions, stored on at least one of the one or more storage devices, to determine whether there is a requirement for authentication for user access to the application; and wherein the program instructions to assign numerical weights to the respective determinations assign a numerical weight to the determination whether there is a requirement for authentication for user access to the application; and the program instructions to combine the numerical weights to quantify the security risk also use the numerical weight for the determinations whether there is a requirement for authentication for user access to the application, in quantifying the security risk.

> *[see col. 8, lines 1-14, wherein Voss teaches that a normal user who exploits a vulnerability might have additional control to see and/or delete other person's data that he or she would not otherwise have]*

As per claim 40, 46:

The computer program product of claim 38 further comprising:

program instructions, stored on at least one of the one or more storage devices, to determine whether a third party can obtain unauthorized administrative authority to data maintained by the application; and program instructions, stored on at least one of the one or more storage devices, to determine whether a third party can obtain unauthorized read and/or write access to data maintained by the application; and wherein the program instructions to assign numerical weights to the respective determinations assign a numerical weight to the determination whether a third party can have unauthorized administrative authority to data maintained by said application, and assign a numerical weight to the determination

whether a third party can have unauthorized read and/or write access to data maintained by said application; and the program instructions to combine the numerical weights to quantify the security risk also use the numerical weight for the determinations whether a third party can have unauthorized administrative authority to data maintained by said application and the numerical weight for the determination whether a third party can have unauthorized read and/or write access to the data, in quantifying the security risk.

[see col. 4, lines 42-52, wherein establishing a numerical value includes identifying one or more unauthorized privileges such as super user read privileges.] see also col. 7-8]

As per claim 41, 47:

The computer program product of claim 38 further comprising:

program instructions, stored on at least one of the one or more storage devices, to determine whether data accessible by a user via the application is confidential; the program instructions to assign numerical weights to the respective determinations assign a numerical weight to the determination whether data accessible by a user via the application is confidential; and the program instructions to combine the numerical weights to quantify the security risk also use the numerical weight for the determinations whether data accessible by a user via the application is confidential.

[see col. 11, unauthorized access to audit logs wherein audit logs are viewed as confidential data]

As per claim 42-43, 48-49:

The computer program product of claim 38 wherein the monetary value of the benefit of the application is a cost savings/revenue gained due to use of the application.

[see Halligan, paragraphs 120-121]

Conclusion

4. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

3. Any response to this Office Action should be **faxed to** (571) 273-8300 **or mailed to**:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Hand-delivered responses should be brought to

Customer Service Window
Randolph Building
401 Dulaney Street
Alexandria, VA 22314

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Daniel L. Hoang whose telephone number is 571-270-1019. The examiner can normally be reached on Monday - Thursday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached at (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Daniel L. Hoang/
Examiner, Art Unit 2436

/Nasser Moazzami/
Supervisory Patent Examiner, Art Unit 2436